CLAIMS

What is claimed is:

1. A method of establishing secure communications in a multi-mode portable communication device, comprising the steps of:

establishing a symmetric traffic key between the multi-mode portable communication device and a second portable communication device in a first mode of communication;

switching to at least a second mode of communication; and

sharing the symmetric traffic key between the multi-mode portable communication device and the second portable communication device.

2. The method of claim 1, wherein the step of establishing the symmetric traffic key is achieved using Automatic Public Key exchange techniques by having the multi-mode portable communication device and the second portable communication device each independently computing the symmetric traffic key using their respective private keys along with a public key of a peer unit before commencing secure communications in a first mode..

3. The method of claim 2, wherein the Automatic Public Key exchange is implemented using public-key algorithms such as Diffie-Hellman cryptography or Elliptic Curve Cryptography.

4. The method of claim 3, wherein the Automatic Public Key exchange is implemented by combining public-key algorithms with a signaling scheme such as Future Narrow Band Digital Terminal protocol.

5. The method of claim 1, wherein the step of switching to the second mode from the first mode comprises switching among modes comprising interconnect voice, dispatch voice, peer-to peer data, and peer-to-peer voice.

6. The method of claim 1, wherein the step of switching to the second mode from the

first mode comprises switching among modes comprising CDMA, TDMA, GSM, and WLAN.

7. The method of claim 1, wherein the method further comprises the step of storing the symmetric traffic key in a phonebook record associated with the second portable communication device.

8. The method of claim 1, wherein the method further comprises the step of storing a predetermined number of symmetric traffic keys in a cache memory associated with a predetermined number of other portable communication devices in recent communication with the multi-mode portable communication device.

9. The method of claim 1, wherein the method further comprises the step of establishing a new communication session between the multi-mode portable communication device and the second portable communication device without requiring an APK key establishment process.

10. The method of claim 1, wherein the method further comprises the step of establishing a key exchange with a plurality of other predetermined portable communication devices during a background mode.

11. A method of establishing secure communications among a plurality of portable communication devices, comprising the steps of:

storing information associated with a predetermined number of other portable communication devices;

establishing a symmetric traffic key using an APK key establishment process between a first portable communication device and the predetermined number of other portable communication devices during a background mode of the first portable communication device; and

establishing a secure communication session between the first portable communication and at least one among the predetermined number of other portable

communication devices without further requiring the APK key establishment process.

12. The method of claim 11, wherein the step of establishing a symmetric traffic key using the APK key establishment process comprises contacting the predetermined number of other portable communication devices to determine if their respective keys have expired and performing a background APK exchange to re-establish a fresh key if the respective key has expired.

13. The method of claim 11, wherein the first portable communication device and the predetermined number of other portable communication devices are multi-mode portable communication devices and the method further comprises the step of establishing a symmetric traffic key between the first portable communication device and at least one among the predetermined number of other portable communication devices in a first mode of communication, switching to at least a second mode of communication, and sharing the symmetric traffic key between the first portable communication device and the at least one among the predetermined number of other portable communication devices in the second mode.

14. A portable communication device capable of operating in multiple modes, comprising:

a transceiver;

a processor coupled to the transceiver, wherein the processor is programmed to:

establish a symmetric traffic key in a first mode of communication between the portable communication device and a second portable communication device;

switch to at least a second mode of communication;

share the symmetric traffic key between the portable communication device and the second multi-mode portable communication device.

15. The portable communication device of claim 14, wherein the processor is programmed to establish the symmetric traffic key using Automatic Public Key

exchange techniques.

16. The portable communication device of claim 15, wherein the Automatic Public Key exchange is implemented using a signaling scheme such as Future Narrow Band Digital Terminal protocol combined with public-key algorithms such as Diffie-Hellman cryptography or Elliptic Curve Cryptography.

17. The portable communication device of claim 14, wherein the processor is programmed to switch to the second mode from the first mode by switching among modes comprising interconnect voice, dispatch voice, peer-to peer data, peer-to-peer voice, CDMA, TDMA, GSM, and WLAN.

18. The portable communication device of claim 14, wherein the processor is further programmed to store the symmetric traffic key in at least one among a phonebook record associated with the second portable communication device and a cache memory associated with a predetermined number of other portable communication devices in recent secure communication with the portable communication device.

19. The portable communication device of claim 14, wherein the processor is further programmed to establish a new communication session between the portable communication device and the second portable communication device without requiring an APK key establishment process.

20. The portable communication device of claim 14, wherein the processor is further programmed to establish a key exchange with a plurality of other predetermined portable communication devices during a background mode.

21. A portable communication device capable of operating in multiple modes, comprising:

a transceiver;

a processor coupled to the transceiver, wherein the processor is programmed to:

store information associated with a predetermined number of other portable communication devices;

establish a symmetric traffic key using an APK key establishment process between a first portable communication device and the predetermined number of other portable communication devices during a background mode of the first portable communication device;

establish a secure communication session between the first portable communication and at least one among the predetermined number of other portable communication devices without further requiring the APK key establishment process.